Open Science Repository Mathematics Online, no. open-access (June 28, 2014): e45011817. doi:10.7392/openaccess.45011817

.

Fermat Primes Cardinality

-By: Alberto Durán-
otreblam@gmail.com
University J.M.Vargas- Faculty: Engineering/Education
Caracas – Venezuela

Abstract: We attempt to show that, there are infinitely many Fermat Primes, by using Schröder - Bernstein's Theorem, another known results in Arithmetic and Number Theory.

Keywords. Fermat Primes(Quadratics Forms), Fermat Primes(classic forms), Pomerance`s Theorem, Cantorian Set Theory.

SMC 2010: 11AXX

1. Introduction.

Leonhard Euler (1707-1783) showed that P. Fermat (1601-1665), was wrong about primality of the number F_5; this fact is so well known, that we not need insist on it$[7]$.In any way, accordingly Historians of Mathematics.P de Fermat it' is justly considered a pioneer theorist in Number Theory$[12]$.It's well known today that, English Mathematician,Dr.Andrew Wiles,proved(1994),the famous marginal note so-called "Fermat Last'sTheorem, namely justly Fermat-Wiles Theorem$[13]$.

2. Notation and Assumptions.

2.1 Starting with, we need distinguishing Fermat Primes (**classic form**) their Fermat Primes (**quadratic form**). More formally, as is usual in Number Theory we will denote Fermat Primes by employing the set below:

$$(1)\quad F_n=\left\{f\in\mathbb{N}: f=2^{2^n}+1,\ \text{where } n\in\mathbb{N} \text{ and } f \text{ is prime}\right\},\ [18].$$

Whereas the symbol Q_p^f denotes Fermatian Primes or **quadratic forms**, this subset of $\mathbb{N}$ plays an very important role in our proof. In such case, we can write more explicitly,

$(2)\quad Q_p^f=\left\{x\in\mathbb{N}: x=n^2+1, n\in\mathbb{N}\right\}$, but x is to be a prime number.

2.2 For the sake of completeness, also we need assume (without proof) some known results in Arithmetic, Algebra and Set Theory:

Lemma 1. Schröder – Bernstein's Theorem.

Let $F:\Phi \to \mho$ and $G:\mho \to \Phi$ be injective functions, then there exists a Biyective function $\Theta:\mho \to \Phi$, $[4]$.

Lemma 2. Cantor's Theorem.
If $\Psi : S \to T$ is a biyective function, thus $Card.(S) = Card.(T)$, $[2]$.
Lemma 3. Pomerance`s Theorem. Every prime p, has a proof of its primality, [5].

3. Preliminary Statements.

3.1.- Before comming to the proof, we need build a natural generating function in the following way; Let $\varphi : \mathbb{N} \to \mathbb{N}$ be defined by the formula below:

(1) $$\varphi(n) = \begin{cases} 2^{2^n}+1 \text{ if and only if } 2^{2^n}+1 \text{ is prime} \\ \mathrm{n}^2+1 \quad \text{otherwise} \end{cases}$$

Proposition 3.1. The set of images of the function $\varphi(n)$, namely I_φ, does contain in particular two infinite subsets: Fermat Primes F_n and $\mathbb{N} - F_n = Q_p^f$, where Q_p^f represents the natural sequence of primes defined at (2) above.
Proof.
Firstly, we must prove the fact that, Q_p^f is not finite.

Notice that, recently (in the twenty one century) has been proved that $Card.(Q_p^f) = \aleph_0$, [3].
Further, in particular Q_p^f contains all Fermat Primes (**quadratic forms**) and we may write: $Q_p^f \subset I_\varphi$, whenever I_φ, stands for the set of images of the function $\varphi(n)$ defined at (1), from this we can see,
(2) $Card.(Q_p^f) = \aleph_0$, as asserted.

3.2 Next, we are going to prove our main result: $Card.(F_n)$ is not finite $[11]$. In order to solve our guess, let I_n be a auxiliary set: $I_n = \{x \in \mathbb{N} : x = 2^n, n \in \mathbb{N}\}$.
Obviously, $Card.(I_n) = \aleph_0$, and by construction, one has the relation:

(3) $Card.(I_n) = Card.(Q_p^f) = Card.(\mathbb{N}) = \aleph_0.$
In the rest of this short article, $L_N x$ means: Logarithm natural of x, $[20]$.

We shall use the following properties of I_n: every $x \in I_n$ can be written by using the set Q_p^f . Of course, we can proceed in the following way:
Let x an arbitrary member of Q_p^f, thus we have that Diophantine equation:

(4) $x = n^2 + 1$ for some $n \in \mathbb{N}$, hence we can write : $x - 1 = n^2$, so one has,

(5) $n^2 = x - 1 \Rightarrow \left[\left(L_N n \right)^{-1} . L_N \left(x - 1 \right) \right]^n = 2^n \in I_n$.

In fact, we have **infinite possibilities** for the choice of n belonging to Q_p^f.

Furthermore, from (4) we can see, $x = n^2 + 1 \Rightarrow n = \left(x - 1 \right)^{1/2}$ consequently,

(6) $2^n = 2^{\sqrt{x-1}} \Rightarrow 2^{2^n} = 2^{2^{\sqrt{x-1}}}$, that is to say; $2^{2^{\sqrt{x-1}}} = 2^{2^n}$, therefore we have,

(7) $2^{2^{\sqrt{x-1}}} + 1 = 2^{2^n} + 1 = f \in F_n$, which tell us that $f \in F_n$ or not, according to for

when $x \in Q_p^f$.This assertion has unique answer computationaly (in accordance with Lemma 3 above or Pomerance´s Theorem).

Unfortunately, not all Fermatian Primes (**quadratic forms**) generates Fermat's Primes, which we need prove the following statement:

Proposition 3.2 Let $\psi_1 : I_n \to F_n$ and $\psi_2 : F_n \to I_n$, be defined by the system,

(8) $$\begin{cases} \psi_1(x) = 2^x + 1 = 2^{2^n} + 1 \\ \psi_2(f) = \log_2(f - 1) \end{cases}$$

Then ψ_1 and ψ_2, so constructed are both injective functions.

Proof.

2.i.- Let us assume that x_1, x_2 both belong to I_n, whence there are natural numbers n_1, n_2 such that :

(9) $x_1 = 2^{n_1}$, and at the same time, $x_2 = 2^{n_2}$, suppose $\psi_1(x_1) = \psi_1(x_2)$, next $2^{2^{n_1}} + 1 = 2^{2^{n_2}} + 1 \Rightarrow 2^{2^{n_1}} = 2^{2^{n_2}}$, from this we may write: $2^{n_1} = 2^{n_2}$ or $x_1 = x_2$.

Thence, we have obtained that ψ_1 is an injective function, as asserted.

2.i.i. Analogously, let us f_1 and f_2 belonging to F_n. We can assume that $f_1 \neq f_2$ and $f_1 < f_2$ (or $f_2 < f_1$, the treatment is the same,(without changing it in any essential way).

According to our hypothesis we can write the following immediate inequalities:

(10) $f_1 - 1 < f_2 - 1$, because f_1 and f_2 are both positive numbers, thus we obtain the relation, $\log_2(f_1 - 1) < \log_2(f_2 - 1)$, but by applying (8), this last inequality takes the form below:

(11) $\psi_2(f_1) < \psi_2(f_2)$, clearly we have $\psi_2(f_1) \neq \psi_2(f_2)$, and ψ_2 also is an **Injective function**, which completes the proof of the Proposition 3.2.

4. Important Results.

4.1. - Finally we can pay attention to our aim in this brief research work.

Proposition 4.1: $Card.(F_n) = \aleph_0$. To prove this statement is sufficient to study carefully the cardinality of the sets F_n and Q_p^f simultaneously. In fact, can occur only four possibilities:

Case 1: If F_n and Q_p^f are both finite sets; in particular Q_p^f should be finite, but we have proved at Proposition 3.1 that $Card.(Q_p^f) = \aleph_0$, therefore we have obtained a contradiction, so this case is not possible.

Case 2: If Q_p^f is infinite and F_n finite. Since F_n is finite, it follows that there exists a biggest Fermat Prime says,

$f_{n^*} = 2^{2^{n^*}} + 1$, for some huge number $n^* \in \mathbb{N}$. This means that:

$\forall n > n^*$, numbers of the form $f_n = 2^{2^n} + 1$ are all composite, therefore, we may write that increasing and **finite** sequence:

(12) $f_1, f_2, f_3, ..., f_{i-1}, f_i, f_{i+1}, ..., f_\lambda$. It is obvious that, by hypotheses the relation

(13) $Card.(F_n) = \lambda \in \mathbb{N}$, holds.

4.2.- Recall that $\psi_1 : I_n \to F_n$ and $\psi_2 : F_n \to I_n$ are both injective functions (Proposition 3.2); then there exists a **Bijective** function $\theta : I_n \to F_n$, by using Lemma 1 or Schröder-Bernstein's Theorem , this is same thing as say that,

(14) $Card.(F_n) = Card.(I_n)$, in accordance with Lemma 2 or Cantor's Theorem.

Clearly (14) contradicts (13), because we have stated at (3) that $Card.(I_n) = \aleph_0$, also this case must be naturally discarded.

Case 3: Assume F_n infinite and Q_p^f is finite. Similarly to Case 1, we have again a contradiction with Proposition 3.1 above.

4.3. - At this point of the proof, all that remains is to discuss the last possibility:

Case 4: When F_n and Q_p^f are both infinite sets. This Hypotheses does not contradicts, any of the previous Theorems or assumptions made in this notes.

However, taking into account that, all possible cases have been examined, we conclude that, sequence of primes of the form $f_n = 2^{2^n} + 1$ never ends; this is another way of saying that, Fermat's Prime numbers go on forever, therefore:
(15) $Card.(F_n) = \aleph_0$, as was to be proved.

5. Concluding comments

In the current literature [6], the higher Fermat numbers have been the subject of prolonged study, to date no more primes have been found among them $[8][23]$.
In other words, $\mathbf{F_n}$ generates primes and composite numbers at random.
Although, we believe that, the next Fermat prime (for **n** greater than 5) would be a so huge number $[21][22]$ and probably our modern computers [9], don't have sufficient memory capacity to contain it $[15][17]$.

6. Acknowledgements

El Autor de este modesto aporte, expresa las más sinceras gracias, a la **Dra. Alicia Fernanda Parra de Ortiz**, **Presidenta del Consejo Superior de la Universidad;**

por todo su apoyo Logístico , para la culminación del presente logro académico.

Así mismo quiero destacar, el constante respaldo moral, por parte de la Prof. y Colega:

PhD. Clara González Silva, quien tiene a su cargo, la **Dirección de Investigación y Proyectos de la Universidad José María Vargas** /Caracas-Venezuela.

7. References

[1] Andrews G.E, (1994). " Numbers Theory " Dover Publications, N.C New York- U.S.A, pags. 65-66

[2] Birkoff G and MacLane S, (1973). " A survey of Modern Algebra " Printed in U,S,A. MacMillan Company. Pags. 361-363

[3] Duràn Alberto, (2002). " The Cardinality of Primes $n^2 + 1$" **iJMEST,**Vol 33, issue # 6 Editorial group, Taylor and Francis. England United Kingdom. Pags. 907-910.

[4] Mostow G.D, Sampson J.H and Mayer J.P, (1963). " Fundamental Structures of Algebra ", MacGraw Hill, New York-U.S.A, pags. 510-513.

[5] Pomerance Carl, (1987). " Every Prime p has a proof of its Primality " **Math. of Computation**, Vol 48- issue 177. AMS, pags. 315-322

[6] Stanley Ogilvy C, (1994). “ Excursions in Number Theory “ Dover Publications, I.N.C, New York-U.S.A, pags. 20-23

[7] Shanks Daniel, (1962).” Solved and Unsolved Problems in Number Theory “. Vol 1, Washington D.C, Spartan Books-USA.

[8] Ribemboim Paul, (1995), The New Book of Prime Numbers Records . Springer Verlag, New York-USA, QA246.R472.

[9] Romely R.S, Adleman R.E & Pomeran C, (1983), On distinguishing prime numbers from composite numbers.Pags. 117-123, QAnn Math.

[10] Waldschmidt Michel, (2004).” Open Diophantine Problems “.Moscow Mathematics Journal,Vol 4, number 1. January-March. Independent University of Moscow. (From English translation), Pages. 245-305.

[11] Wallace D.F, (2003). “ Everything and More: A Compact History of Infinite”. Norton and Company ISBN 0-393-00338-8.New York-USA

[12] Weil A ,(1984). “ Number Theory : An approach through History “ Birkhâuser, Basel-Swiss.

[13] Williams H.C, (1998). Edoard Lucas and Primality Testing, John Wisley and Sons, INC. New York-USA.

[14] Wiles, A. "Modular Elliptic-Curves and Fermat's Last Theorem." *Ann. Math.* **141**, 443-551, 1995.

[15] Parady B.K, Smith T.S & Zarantonello S.E, (1990), Largest known Twin Primes, Math.of Comp. **55**.Pags.382-383, Published by AMS.

[16] Pomerance Carl, (1987). Every prime p has a proof of its Primality. Math. of Comp.Vol 48, issue **177**.Pages.315-322, Published by AMS.

[17] Romely R.S, Adleman R.E & Pomeran C, (1983), On distinguishing prime numbers from composite numbers. Pags.117-123, QAnn Math.

[18] Well David, (1997), The Penguin of Curious and interesting numbers, revised edition. Penguin Books Ltd, registred office Strand-England United Kingdom. Pag. 134-135.

[19] Weil, André (1967), Basic number theory. Die Grundlehren der mathematischen Wissenschaften 144, Springer-Verlag New York, Inc., New York, USA.

[20] Wittaker E.T & Watson G.N, (1963). A Course in Modern Analysis, four edition, Cambridge University Press, ISBN.0-521-58807-3, N.Y-USA.

[21] Yates S, (1992).Collecting gigantic and Titanic Primes,J Recreational Math. p.193-201.New York, USA.

[22] Zagier Don, (1977).The first 50 Million Prime Numbers, Math.Intelligencer, August, Pages.7-19.New York, USA.

[23] Zinmmermann P, (2002) Ten Consecutive Primes in Arithmetical Progression, Math. of Comp.**71**:239. p.1323-1328. New York.